ABSTRACT

The invention provides for a cryptographic method for digital signature.

A set S1 of k polynomial functions $P_k(x_1,\ldots,x_{n+v}, y_1,\ldots,y_k)$ are supplied as a public key, where k, v, and n are integers, $x_1,\ldots,x_{n+v}$ are n+v variables of a first type, and $y_1,\ldots,y_k$ are k variables of a second type, the set S1 being obtained by applying a secret key operation on a given set S2 of k polynomial functions $P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$, $a_1,\ldots,a_{n+v}$ designating n+v variables including a set of n "oil" and v "vinegar" variables.

A message to be signed is provided and submitted to a hash function to produce a series of k values $b_1,\ldots,b_k$. These k values are substituted for the k variables $y_1,\ldots,y_k$ of the set S2 to produce a set S3 of k polynomial functions $P''_k(a_1,\ldots,a_{n+v})$, and v values $a'_{n+1},\ldots,a'_{n+v}$ are selected for the v "vinegar" variables. A set of equations $P''_k(a_1,\ldots,a'_{n+v})=0$ is solved to obtain a solution for $a'_1,\ldots,a'_n$ and the secret key operation is applied to transform the solution to the digital signature.